European Journal of Computer Science and Information Technology, 13(48),33-44, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

AI-Driven Cloud Solutions for Anti-Money Laundering (AML) Compliance with Graph Neural Networks and Behavioral Analytics

Siva Prakash
Bharathidasan University, India

doi: https://doi.org/10.37745/ejcsit.2013/vol13n483344 Published July 02, 2025

Citation: Prakash S. (2025) AI-Driven Cloud Solutions for Anti-Money Laundering (AML) Compliance with Graph Neural Networks and Behavioral Analytics, *European Journal of Computer Science and Information Technology*, 13(48),33-44

Abstract: *This article examines the integration of artificial intelligence with cloud computing to transform anti-money laundering compliance in financial institutions. Traditional rule-based AML systems have proven inadequate against sophisticated financial crimes, generating excessive false positives while missing complex schemes. Graph Neural Networks offer unprecedented capability to analyze transaction networks by modeling relationships between entities and detecting anomalous patterns. Behavioral analytics complements this approach by focusing on temporal patterns of individual customers, enabling dynamic risk profiling based on transactional behavior rather than static attributes. The cloud infrastructure supporting these analytics provides the necessary computational scalability, data integration capabilities, and real-time processing essential for modern AML operations. Implementation considerations include model explainability, regulatory compliance, and data protection requirements. The article explores emerging trends including federated learning for cross-institutional collaboration and advanced natural language processing for unstructured data analysis. This technological convergence represents not merely an incremental improvement but a fundamental transformation in AML capabilities, enabling financial institutions to implement sophisticated detection algorithms at scale while maintaining regulatory compliance and operational efficiency.*

Keywords: graph neural networks, behavioral analytics, cloud computing, anti-money laundering, financial crime detection

INTRODUCTION

Money laundering continues to pose significant challenges to the global financial system, with substantial portions of global GDP being laundered annually. These figures represent a conservative assessment based

on empirical analyses of illicit financial flows conducted across multiple jurisdictions, highlighting the pervasive nature of financial crime within global economic systems. According to comprehensive studies documented in the Sea Open Research Journal, financial crime patterns have evolved substantially over recent years, with marked increases in sophisticated layering techniques and greater utilization of virtual assets to obscure money trails [1]. Traditional rule-based anti-money laundering (AML) systems have demonstrated insufficient efficacy against these increasingly sophisticated financial crimes, generating high false positive rates in production environments and necessitating considerable person-hours per case for manual investigation.

Financial institutions face intensifying regulatory pressure to enhance their AML compliance programs while simultaneously managing operational costs. Global spending on AML compliance infrastructure and operations has followed a steep upward trajectory, with total expenditure projected to increase significantly in coming years. The regulatory landscape has similarly evolved, with AML-related enforcement actions increasing and the average monetary penalty per action rising during recent periods, reflecting heightened regulatory expectations and scrutiny regarding AML compliance effectiveness [1]. This escalating cost structure has created urgent incentives for financial institutions to adopt more efficient and effective AML methodologies.

The field of Anti-Money Laundering (AML) technology is rapidly evolving, with emerging techniques promising to revolutionize financial crime detection. Explainable AI for Graph Neural Networks is pushing the boundaries of model interpretability, moving beyond traditional feature importance metrics to provide structural and contextual explanations of how complex financial networks are analyzed. These advanced techniques aim to create "glass box" models that maintain high detection accuracy while offering transparent reasoning for each generated alert.

Artificial intelligence (AI) has emerged as a transformative technology in AML compliance, offering enhanced detection capabilities, improved operational efficiency, and reduced false positives. Detailed research published in the Social Science Research Network has documented that financial institutions implementing advanced AI-based AML solutions experience substantial reductions in false positives while simultaneously achieving significant increases in true positive detection rates compared to traditional rule-based systems [2]. These improvements translate directly to operational efficiencies, with case investigation times reduced due to more precise alert generation and enhanced contextual information. This systematic performance improvement has been validated across multiple financial sectors, with retail banking, commercial banking, and investment banking segments all demonstrating statistically significant enhancements in detection accuracy following AI implementation [2].

Table 1: Traditional AML vs. AI-Enhanced AML Solutions [2]

Feature	Traditional Rule-Based Systems	AI-Enhanced Solutions
Detection Approach	Static rules and thresholds	Dynamic, contextual risk assessment
False Positive Rate	High	Significantly reduced
Investigation Efficiency	Time-consuming manual review	Streamlined with contextual information
Detection Capability	Known patterns only	Known and emerging patterns
Analysis Methods	Rule matching	Graph analysis and behavioral modeling
Adaptability	Manual updates required	Self-improving through feedback
Processing Mode	Batch processing	Real-time monitoring
Documentation	Manual	Automated with explainability

Graph Neural Networks for Financial Crime Detection

Graph Neural Networks (GNNs) represent a significant advancement in the application of deep learning to networked data structures. Unlike conventional neural networks that process individual data points in isolation, GNNs explicitly model relationships between entities, making them uniquely suitable for analyzing the complex networks of transactions and relationships characteristic of financial systems. The Social Science Research Network has published comprehensive analyses demonstrating that GNN-based AML systems significantly outperform traditional machine learning approaches, with documented performance improvements across multiple evaluation metrics when applied to large financial transaction networks [2]. These performance improvements stem primarily from the ability of GNNs to leverage both entity-level features and the structural properties of transaction networks simultaneously, capturing subtle patterns that remain invisible to conventional modeling approaches.

Behavioral analytics is undergoing a significant transformation through the integration of causal inference techniques. Unlike traditional correlation-based approaches, this new methodology seeks to understand the fundamental drivers of suspicious financial behavior. By employing structural causal models, intervention analysis, and counterfactual reasoning, financial institutions can now distinguish between coincidental patterns and causally significant behavioral shifts, providing more nuanced and insightful risk assessments.

Theoretical Foundations of GNNs in AML

The theoretical foundations of GNNs as applied to AML contexts build upon established graph theory while incorporating modern deep learning principles. These networks extend traditional neural network architectures by incorporating graph structures, enabling them to learn representations that capture both node features and the topology of connections. In typical AML implementations, each node in the graph represents an entity (customer, account, or transaction), while edges represent relationships or interactions

between entities, such as payment flows, shared ownership structures, or other meaningful connections. GNNs employ sophisticated message-passing mechanisms to propagate and aggregate information across the graph, allowing the model to capture multi-hop dependencies and complex patterns of behavior that frequently characterize money laundering operations. Research published in the European Union's Anti-Money Laundering Digital Transformation initiative has documented that effective GNN implementations typically utilize multiple message-passing layers, allowing the model to capture dependencies spanning several degrees of separation within the transaction network [3].

The mathematical formulation of a GNN layer can be expressed as $H^{(l+1)} = f(H^{(l)}, A)$, where $H^{(l)}$ represents the node features at layer l, A represents the adjacency matrix of the graph, and f is a differentiable function that updates node representations based on their neighborhood information. In practical AML implementations, this formulation is frequently extended to incorporate edge features and temporal dynamics, resulting in more sophisticated architectures such as Temporal Graph Convolutional Networks and Relational Graph Attention Networks. Benchmark evaluations conducted across major European financial institutions have demonstrated that these advanced GNN variants achieve significantly higher precision scores compared to traditional machine learning approaches when identifying synthetic money laundering patterns in transaction networks [3]. This substantial performance differential underscores the transformative potential of graph-based deep learning approaches for AML applications.

Network Analysis for Suspicious Activity Detection

GNNs demonstrate exceptional efficacy in detecting money laundering typologies that involve complex networks of transactions designed to obscure the origin of illicit funds. Empirical research documented in Sea Open Research has identified several distinctive structural patterns frequently associated with money laundering operations, each of which can be effectively detected through graph-based analytical approaches [1]. Layering schemes, where funds pass through multiple intermediaries to obscure their source, typically exhibit characteristic chain lengths in sophisticated money laundering operations based on analysis of confirmed cases across multiple jurisdictions. These sequential transaction patterns often incorporate specific timing characteristics, with the majority of identified layering schemes executing the complete transaction sequence within short timeframes, creating a distinctive temporal signature that can be captured by temporal GNN variants.

Smurfing patterns involving numerous small transactions converging to a central account represent another prominent money laundering typology readily detectable through graph analysis. Detailed examinations of transaction networks have revealed that mature smurfing operations typically involve multiple source accounts making transactions below regulatory thresholds, with these operations exhibiting transaction amounts clustering near relevant reporting thresholds [1]. The structural signature of these operations—a convergent star-like pattern with temporal coordination—creates a distinctive subgraph structure that GNN models can identify with high precision. Analysis of confirmed money laundering cases has revealed that a significant portion of major money laundering schemes involve circular transaction patterns where funds

circulate through a closed loop of accounts, creating another identifiable structural pattern that graph-based approaches are uniquely positioned to detect.

Table 2: Money Laundering Patterns Detectable by Graph Neural Networks [1]

Pattern Type	Description	Key Network Characteristics
Layering	Funds passing through multiple intermediaries	Chain-like transaction paths
Smurfing	Small transactions converging to central account	Star-like pattern below thresholds
Circular Transfers	Funds circulating through account loops	Cycle structures in transaction graph
Shell Company Networks	Entities with limited business purpose	Hub-and-spoke with minimal history
Beneficial Ownership	Hidden ultimate owners	Nested ownership structures

Implementation Challenges and Solutions

Implementing GNNs for AML presents several significant challenges that must be addressed to achieve optimal performance. Primary among these are graph construction from transactional data, handling temporal dynamics, and scaling to massive financial networks comprising numerous nodes and edges. Research published in Heliyon has systematically documented these implementation challenges along with viable solution approaches, providing a roadmap for effective GNN deployment in production AML systems [4]. The computational requirements for training and inference with large-scale graph models have traditionally presented a significant barrier to adoption, but cloud-based solutions effectively address these challenges through several mechanisms.

Distributed graph processing frameworks such as Apache GraphX and TensorFlow Graph Neural Networks provide the computational infrastructure necessary for operating on massive financial networks. These frameworks have demonstrated the ability to process extremely large graphs on standard cloud infrastructure, with linear scaling properties that maintain performance as data volumes grow [3]. This scalability is essential given the size of modern financial networks—a typical global bank may process millions of transactions daily, creating a dynamic transaction graph that grows by many millions of edges monthly. Temporal GNN variants explicitly model the evolution of financial relationships over time, capturing substantially more suspicious patterns compared to static graph approaches according to comparative studies conducted across multiple financial datasets spanning years of transaction history [3].

European Journal of Computer Science and Information Technology, 13(48),33-44, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Behavioral Analytics for Customer Risk Profiling

Behavioral analytics complements network-based approaches by focusing on the temporal patterns of individual customers and accounts. This methodology represents a paradigm shift from static, demographic-based risk assessment toward dynamic profiling based on transactional behavior and activity patterns. Research published in Heliyon has documented the effectiveness of this approach, demonstrating that behavioral analytics systems capture significantly more suspicious activity cases than traditional rules-based systems while simultaneously reducing false positive rates across diverse financial institutions [4]. These performance improvements derive from the fundamental premise that anomalous behavior, rather than static attributes, provides the most reliable signal of potential money laundering activity.

Advanced learning approaches are reshaping how financial institutions approach anomaly detection. Self-supervised learning techniques are enabling pre-training of models on large-scale transactional data without extensive manual labeling, capturing intricate behavioral patterns with unprecedented precision. Simultaneously, hybrid AI architectures are emerging, combining Graph Neural Networks with Transformer models to create holistic approaches that capture both network structure and sequential behavior through dynamic attention mechanisms.

Customer Behavior Modeling Techniques

Modern behavioral analytics employs a sophisticated array of techniques to establish baseline customer behavior and detect deviations that may indicate money laundering or other financial crimes. Unsupervised clustering of customers based on transaction patterns, frequency, and amounts represents a foundational approach, with optimal implementations identifying distinct behavioral clusters across retail banking populations according to research published in the European Union's Anti-Money Laundering Digital Transformation initiative [3]. These behavioral clusters capture natural groupings in customer transaction patterns, with cluster membership evolving dynamically as customer behavior changes over time. The resulting behavioral segmentation provides substantially greater resolution than traditional demographic segmentation, with studies demonstrating significant improvement in homogeneity of transaction patterns within behavioral segments compared to demographic segments.

Sequence modeling with recurrent neural networks enables the capture of temporal dependencies in transaction histories, providing crucial context for determining whether current activity represents a natural evolution of established patterns or a potentially suspicious deviation. Longitudinal studies across financial institutions have documented that temporal modeling reduces false positives compared to non-temporal models while maintaining or improving true positive rates [2]. These improvements stem from the ability of sequence models to distinguish between legitimate changes in customer behavior—such as seasonal patterns, life events, or evolving business activities—and the abrupt or uncharacteristic changes frequently associated with account compromise or money laundering activity. Practical implementations typically utilize Long Short-Term Memory (LSTM) or Transformer architectures operating on transaction sequences spanning many months, with sliding window approaches enabling continuous updating of behavioral profiles as new transactions occur.

Contextual Anomaly Detection

Behavioral analytics demonstrates particular effectiveness in identifying contextual anomalies—activities that appear normal in isolation but become suspicious when considered against the customer's established patterns or peer group behavior. These systems consider multiple contextual factors to determine whether a transaction or activity pattern warrants further investigation. Historical transaction patterns for the specific customer typically form the primary baseline for anomaly detection, with research published in Sea Open Research establishing that effective implementations analyze sufficient transaction history to establish reliable behavioral baselines, with the optimal window varying based on customer type and transaction frequency [1]. For retail customers, shorter periods typically provide sufficient historical context, while commercial banking relationships often require longer timeframes to capture the full range of normal business activities and cycles.

Peer group analysis provides an additional contextual dimension, comparing customer behavior not only against their own history but also against similar customers or accounts. According to comprehensive studies documented in the European Union's Anti-Money Laundering Digital Transformation initiative, these peer groups typically comprise many accounts with similar demographic and transactional characteristics, with dynamic peer group assignment recalculated regularly to reflect evolving customer relationships and behaviors [3]. This multi-dimensional approach to anomaly detection enables the identification of activities that might appear normal in the context of the individual customer's history but represent significant deviations from peer behavior, or vice versa. Business purpose and expected activity assessments provide further context, with deviation thresholds calibrated based on analysis of extensive customer-months of transaction data spanning diverse account types and business categories.

Integration with Traditional AML Systems

Rather than replacing existing AML infrastructure, behavioral analytics complements and enhances traditional systems through strategic integration points that maximize the combined effectiveness of multiple detection approaches. Pre-screening transactions to prioritize high-risk alerts for manual review represents a particularly effective integration strategy, with implementations documented in the Social Science Research Network reducing alert volume substantially while maintaining or improving detection rates [2]. This screening approach applies behavioral and network models as a secondary filter on alerts generated by traditional rule-based systems, substantially reducing the investigation burden while ensuring that potentially suspicious activities continue to receive appropriate scrutiny. The resulting workflow optimization enables compliance teams to focus their resources on the most promising cases, significantly enhancing operational efficiency.

Behavioral analytics further enhances investigation efficiency by providing additional context and risk factors for alert investigation. Research conducted across multiple financial institutions found that incorporating behavioral context decreased average investigation time per case while simultaneously improving investigation quality as measured by supervisor review scores [2]. This efficiency gain stems from the ability of behavioral models to provide investigators with relevant historical patterns, peer

comparisons, and specific anomaly indicators that focus the investigation on the most relevant aspects of the case. Rather than manually assembling this context from disparate systems, investigators receive comprehensive behavioral profiles that highlight the specific factors contributing to the risk assessment, streamlining the investigation process.

Cloud-Based Data Architecture for AML Analytics

The effectiveness of AI-driven AML solutions depends critically on the underlying data architecture. Cloud platforms offer robust, scalable infrastructure for managing the diverse, high-volume data required for comprehensive AML analysis. Research published in the World Journal of Advanced Research and Reviews has documented that financial institutions implementing cloud-based AML solutions experienced significant reduction in false positive rates and substantial improvement in suspicious activity detection compared to on-premises deployments of equivalent algorithms. Cloud-based implementations achieve these improvements while processing millions of transactions daily—volumes that would overwhelm most traditional infrastructure deployments [5]. This performance differential highlights the transformative potential of cloud-based architectures for AML applications, enabling financial institutions to implement sophisticated detection algorithms at scale while maintaining acceptable operational costs.

Generative AI is proving to be a powerful tool in AML model development. These techniques allow for the creation of high-fidelity synthetic transaction data, enabling financial institutions to simulate novel money laundering typologies, augment training datasets with realistic scenarios, and comprehensively test models while preserving data privacy. This approach addresses critical limitations in traditional model training by providing rich, diverse training scenarios that reflect the complexity of financial crime.

Data Integration and Harmonization

Financial institutions typically maintain customer and transaction data across multiple siloed systems, creating substantial challenges for comprehensive risk assessment. Cloud-based data lakes and data mesh architectures facilitate the integration of these disparate sources to create a holistic view of customer activity and relationships. According to research published by the Global Association of Risk Professionals, the typical financial institution maintains several separate systems containing AML-relevant data, with limited integration capabilities between these systems. This fragmentation results in detection gaps that sophisticated money launderers readily exploit, with analysis of confirmed money laundering cases revealing that many cases involved activity spanning multiple data systems that went undetected due to siloed monitoring approaches [6].

The integration challenge extends across a diverse range of data sources, each providing essential context for comprehensive risk assessment. Core banking systems and transaction processing platforms generate the foundational activity data. Customer relationship management systems provide vital contextual information about expected customer behavior and business purpose, enhancing the ability to distinguish between legitimate and suspicious activity patterns. External data sources such as sanctions lists, politically exposed persons registries, and adverse media screening services contribute critical risk indicators, with

modern AML systems typically integrating many distinct external data feeds representing millions of entities of regulatory interest [6].

Scalable Storage Solutions for Complex Financial Data

The volume and complexity of data required for comprehensive AML analysis necessitate specialized storage solutions that traditional relational database architecture cannot efficiently support. Research published in ResearchGate examining AML system architectures found that those implementing specialized cloud storage solutions achieved significant query performance improvements for typical investigative query patterns compared to traditional relational databases [8]. Graph databases provide optimized storage and traversal capabilities for modeling relationship networks, enabling analysts to identify connection patterns that would remain invisible in traditional storage structures. Implementations of graph databases for AML purposes have demonstrated particular value for beneficial ownership analysis, reducing the time required to identify ultimate beneficial owners from hours of manual investigation to seconds of automated graph traversal [8].

Table 3: Cloud Infrastructure for AML Systems [8]

Component Type	Examples	Primary AML Function
Data Storage	Graph databases, data lakes	Multi-source data integration
Processing	Distributed frameworks	Large-scale analysis
Real-time Services	Streaming platforms	Continuous monitoring
Security	Encryption, access controls	Data protection
Analytics	ML platforms, visualization	Model deployment and investigation

Time-series databases offer specialized capabilities for capturing temporal patterns in transaction data, a critical dimension for AML analysis that traditional storage architectures struggle to support efficiently. Research published in the International Journal of Recent Advances in Computer and Information Technology has documented that time-series optimized storage provides substantial query performance improvements for velocity analysis and periodicity analysis compared to general-purpose databases, enhancing detection of sophisticated money laundering schemes that exploit timing patterns to evade traditional monitoring approaches [7].

Implementation Strategies and Regulatory Considerations

The implementation of AI-driven cloud solutions for AML compliance requires careful consideration of technical, organizational, and regulatory factors to ensure effectiveness and compliance. Survey research indicates that while most financial institutions recognize the potential value of AI-enhanced AML, only a fraction have achieved successful enterprise-scale implementations, highlighting the substantial implementation challenges associated with these advanced technologies [5]. Successful implementations typically involve cross-functional teams spanning compliance, IT, data science, and business operations working in close collaboration, with strong executive sponsorship and clearly defined success metrics.

Model Development and Validation

Financial institutions must establish robust processes for developing, validating, and monitoring AI models used in AML compliance. Research examining successful AI-driven AML implementations found that leading organizations allocate significant project effort to data preparation and quality assurance, model development, validation and testing, implementation and integration, and documentation and governance [5]. This allocation reflects the critical importance of data quality for effective model performance, with poor data quality cited as the primary cause of implementation failure in many unsuccessful AI initiatives. The model development process typically begins with comprehensive data quality assessment and feature engineering, establishing the foundation for effective detection algorithms. Research indicates that effective AML models typically incorporate numerous distinct features spanning transaction patterns, customer attributes, network characteristics, and external risk indicators to achieve optimal detection performance [6]. These features require careful engineering and validation to ensure they accurately capture the relevant risk dimensions without introducing biases that might compromise model performance.

Explainability and Regulatory Compliance

Regulatory requirements emphasize the importance of explainable AI in AML applications, creating tension with the complexity of advanced models such as deep neural networks and ensemble methods that often operate as "black boxes." Research analyzing regulatory enforcement actions found that many AML-related penalties included findings related to inadequate model governance or unexplainable detection logic, highlighting the critical importance of explainability for regulatory compliance [5]. Financial institutions must achieve an appropriate balance between model sophistication and transparency, employing various techniques to provide intelligible explanations of model decisions to investigators, auditors, and regulators.

Challenge	Key Issues	Solution Approach
Data Quality	Fragmentation, inconsistency	Harmonization, entity resolution
Explainability	Regulatory requirements	Interpretable AI techniques
Compliance	Model risk management	Validation frameworks, documentation
Privacy	Sensitive data handling	Encryption, data governance
Scalability	Transaction volumes	Cloud-native architecture
Organizational	Skill gaps, process change	Training, phased implementation

Table 4: Implementation Challenges and Solutions [6]

Local interpretability techniques explain individual predictions, providing specific rationales for why particular transactions or customers generated alerts. Effective explanation frameworks typically highlight the most influential factors contributing to each alert, presented in a format that aligns with investigator workflows and domain knowledge [6]. SHAP values have emerged as a particularly effective approach for local explanations, quantifying the contribution of each feature to the final risk assessment and enabling investigators to quickly identify the most relevant risk factors.

Future Directions and Emerging Trends

The field of AI-driven AML compliance continues to evolve rapidly, with several emerging trends likely to shape future developments. Research surveying financial technology innovation identified key areas expected to significantly impact AML capabilities: collaborative approaches spanning multiple institutions, advanced techniques for unstructured data analysis, quantum computing applications, and deeper integration of regulatory technology with AML systems [8]. These trends address fundamental challenges that have historically limited AML effectiveness: information fragmentation across institutions, reliance on structured data, computational limitations, and the operational burden of regulatory compliance.

The future of AML compliance lies in creating holistic, intelligent systems that can detect increasingly sophisticated financial crimes while maintaining transparency, privacy, and adaptability. By integrating advanced AI techniques, privacy-preserving technologies, and sophisticated analytical approaches, financial institutions are moving towards a more proactive and intelligent approach to combating financial crime. These emerging technologies promise to transform AML from a reactive compliance function to a dynamic, predictive intelligence system capable of staying ahead of evolving financial criminal tactics.

Federated Learning for Cross-Institutional Collaboration

Federated learning offers a promising approach for enabling collaboration between financial institutions without sharing sensitive customer data, addressing the challenge that money launderers can exploit information gaps between institutions. Research examining a federated learning pilot found that the collaborative model achieved significant improvement in detection rate for cross-institutional money laundering schemes while maintaining complete data privacy [7]. The federated learning paradigm operates by having each institution train models on local data, sharing only model parameters for aggregation into a consensus model that benefits from the collective knowledge of all participating institutions.

The implementation of federated learning for AML involves specialized components to ensure both effectiveness and privacy protection. Effective implementations typically employ differential privacy techniques that add calibrated noise to model parameters before sharing, preventing reconstruction attacks that might otherwise extract sensitive information [6]. These privacy mechanisms are supplemented by secure aggregation protocols that combine model updates in an encrypted form, ensuring that no participating institution can see another's raw model parameters.

CONCLUSION

The convergence of AI techniques with cloud computing infrastructure represents a watershed moment for anti-money laundering compliance. Graph Neural Networks provide unprecedented capability to analyze complex transaction networks, while behavioral analytics delivers insights into individual customer activity patterns. Together, these approaches create a comprehensive detection framework that substantially outperforms traditional systems. Cloud-based infrastructure delivers the computational scalability, data integration capabilities, and real-time processing essential for implementing these sophisticated

technologies at scale. However, successful implementation requires addressing challenges in model explainability, regulatory compliance, and data protection. Emerging trends including federated learning for cross-institutional collaboration, advanced NLP for unstructured data analysis, quantum computing, and regulatory technology integration promise to further enhance AML capabilities. These developments address fundamental limitations: information fragmentation across institutions, reliance on structured data, computational constraints, and regulatory compliance burdens. As financial crimes grow more sophisticated, this technological transformation provides powerful new tools for detection and prevention. Financial institutions that successfully implement these advanced technologies will not only achieve regulatory compliance more efficiently but also contribute substantively to combating financial crime, terrorist financing, and other illicit activities that threaten the integrity of the global financial system

References

[1] Robert Claudiu HELLVIG, et al, "Impact of globalization on money laundering," SEA, 2023, Online, Available: https://seaopenresearch.eu/Journals/articles/SPAS_32_1.pdf

[2] Jingguang Han, et al, "Artificial Intelligence for Anti-Money Laundering - A Review and Extension," 18 Feb 2021, SSRN, Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3625415

[3] Brian O'Donoghue, "The EU Anti Money Laundering Authority: A Digital Transformation," March 2025, Online, Available: https://www.researchgate.net/publication/389731383_The_EU_Anti_Money_Laundering_Authority_A_Digital_Transformation

[4] Debidutta Pattnaik, et al, "Applications of artificial intelligence and machine learning in the financial services industry: A bibliometric review," 15 January 2024, sciencedirect, Available: https://www.sciencedirect.com/science/article/pii/S2405844023107006

[5] Cedrick Agorbia-Atta and Imande Atalor, "Enhancing anti-money laundering capabilities: The strategic use of AI and cloud technologies in financial crime prevention," World Journal of Advanced Research and Reviews, 2024, Available: https://wjarr.com/sites/default/files/WJARR-2024-2508.pdf

[6] Gary M. Shiffman, et al, "Artificial Intelligence and the Revolution in Financial Crimes Compliance," Anti-Fraud Technology Benchmarking Report, 2022, Available: https://www.garp.org/hubfs/Whitepapers/a2r5d000006RYkPAAW_RiskIntell.WP.Artificial%20Intelligence%20and%20the%20Revolution%20in%20Financial%20Crimes%20Compliance.11.22.pdf

[7] Srinivas Reddy Mosali, "CLOUD-NATIVE ARCHITECTURES IN FINANCIAL SERVICES: A COMPREHENSIVE ANALYSIS OF AI WORKLOAD SCALING AND FRAUD DETECTION," 2025, IAEME, Available: https://iaeme.com/Home/article_id/IJRCAIT_08_01_188

[8] Richard Grint, et al, "NEW TECHNOLOGIES AND ANTI-MONEY LAUNDERING COMPLIANCE," FINANCIAL CONDUCT AUTHORITY 31/03/2017, Available: https://www.fca.org.uk/publication/research/new-technologies-in-aml-final-report.pdf